Open Source Conference 2007 Tokyo/Spring

組み込みセキュアOSの動向

セキュアOSユーザ会
（旧 日本SELinuxユーザ会）
宍道　洋

目次

- 組み込み機器とセキュリティ
- セキュアOSについて
- 主なOSSのセキュアOS
- BusyBoxについて
- 最後に

組み込み機器とセキュリティ

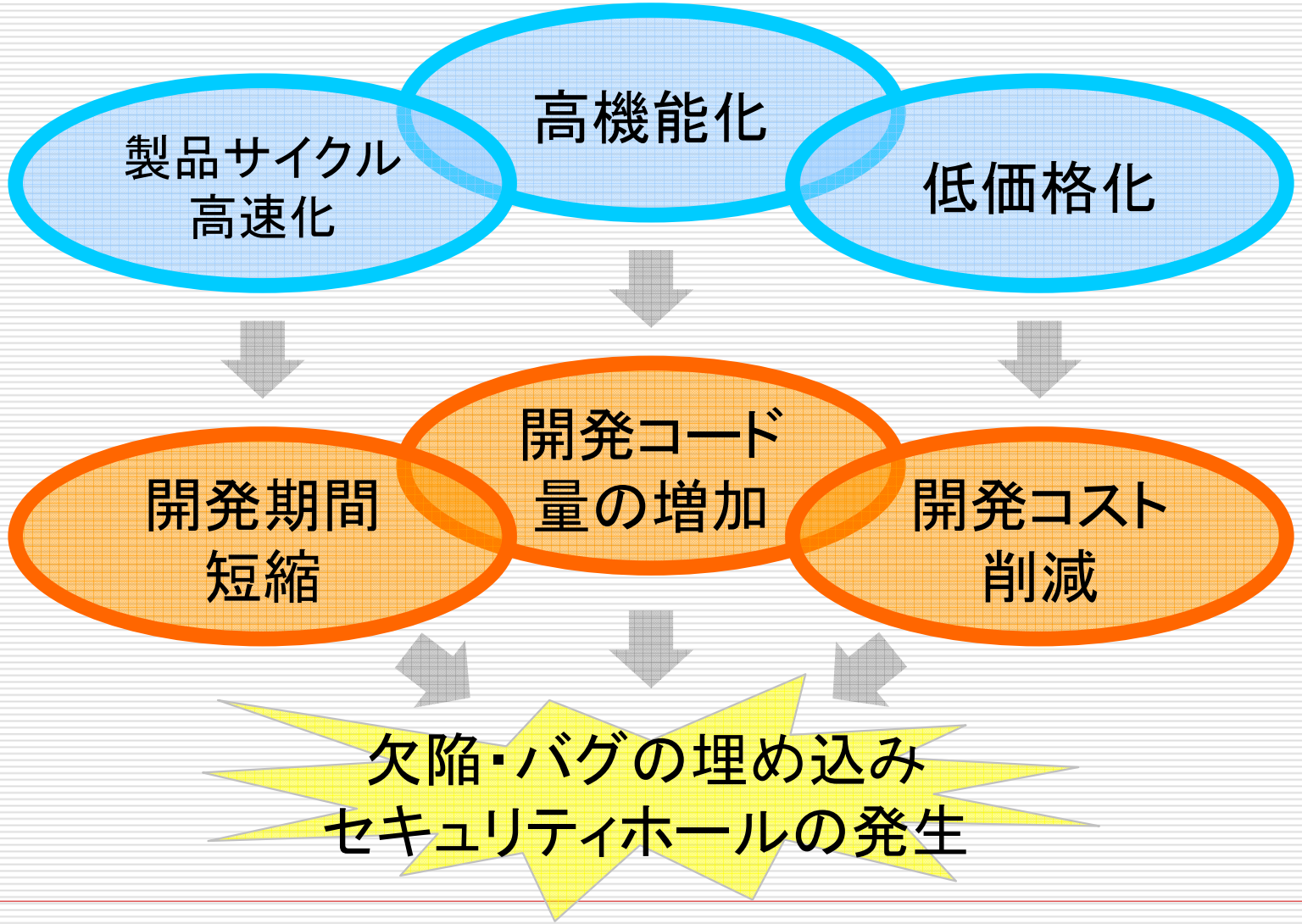
身の回りの組み込み機器

- ケータイ、PHS、PDA
- PC周辺機器、ゲーム機
- TV、オーディオ、HDレコーダ
- 洗濯機、冷蔵庫、炊飯器、電子レンジ
- 自動車、航空機、ロケット、人工衛星
- 計測・制御機器
  - 工場の生産ライン
  - 電力、上水・下水、・・・
    - 供給設備、メータ、などなど

組み込み機器ってどんなもの？

- 必要な機能だけをハードウェア＋ソフトウェアで実現
  - 要求に合わせた最小限のCPU、メモリ、I/O、....
  - ソフトウェアはその機器に特化することが多い
- 要求として・・・堅牢性、信頼性
  - 可動部分（回転系など）を可能な限り減らす
  - 機能が正しく動作すること
- その他
  - 早い起動・停止時間、使い勝手の良さ
  - リアルタイム性能 （制御系など）
  - マルチCPU & マルチOS (RT + UI)
  - 「管理者」「ユーザ」の概念の有無

組み込み機器の傾向


製品サイクル
高速化
高機能化
低価格化
開発期間
短縮
開発コード
量の増加
開発コスト
削減
欠陥・バグの埋め込み
セキュリティホールの発生

セキュリティに対する意識は？

- 組み込み機器開発者のセキュリティ意識は少し前まであまり高くなかった
  - インターネットにつながってないし・・・
  - CPUアーキテクチャがIntel系じゃないし・・・
  - 組み込み機器に好きこのんで攻撃しないでしょ・・・
  - 大したデータはないし・・・
  - なんかセキュリティの設定や試験も面倒だし・・・
  - セキュリティについて考えてる時間ないし・・・

組み込み機器のセキュリティ侵害例

- 情報家電・事務機器など
  - ATMや複合機にウィルス（2003年）
  - 携帯電話（Symbian OS）でのトロイの木馬型ウィルス
    - 2004/06「Cabir」　2004/11「Skulls」
    - その他、多くの亜種
  - HDDレコーダでコメントスパムの踏み台（2004年）
- 産業用システムなど
  - 送電を制御する電力会社のシステムに不正侵入
    - 2001/05頃　米国カリフォルニア州
  - ある生産ラインでのウィルス蔓延
    - ウィルスによるリソース消費 → 生産ラインストップ

（数億円の被害）

組み込み機器の特徴(情報家電など)

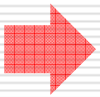
- 利用者の個人情報を格納
- 同じ機器が市場に大量に出回る
  - ひとつの脆弱性による被害が大きくなる可能性
- アップデートが簡単にできない
  - ROMファイルシステム上にアプリが焼かれている場合がある
  - ネットワーク経由でアップデートできるものも増えてきた
    - でも、アップデートしないで使うユーザも多いかも

組み込み機器の特徴(産業用途など)

- 厳しい稼動条件
  - 24時間連続稼動
  - 高信頼性・長寿命設計が要求される
  - 過酷な使用環境(温度／湿度／粉塵 etc.)
- アップデートが簡単に出来ない
  - 生産ラインなどのシステム全体を停止する必要
  - 場合によっては数年～10年以上連続動作

今後起こりうる被害

- 情報漏えい
  - 個人情報、機密情報、著作権管理されたコンテンツの盗難
  - 計測データなど、時系列情報の収集
    - 電気、水道、ガスなど → 住人の在・不在、生活パターン
- 外部からの機器の不正操作
  - 家電や、医療機器、工場のラインが突然動作・停止したり・・・
    - 異常動作による機器の故障、怪我などの人的被害
- 踏み台、外部への攻撃
  - ボットネット、Spamメール、DDoS攻撃
    - 侵入されたかどうか気付きにくい
- 機器の交換・修理のための大量回収など
  - 非常に多くのコストと手間



組み込み機器でも、ウィルス/ワームの感染防止機能や不正侵入対策が必要

セキュアOSについて

セキュアOSの定義

- 最少特権化
  - コンピュータシステム内の主体(ユーザやプログラム)が持つ権限を必要最小限にできること
    - 個々のアプリケーションは、権限を与えられた処理(特定ファイルへのアクセス権限など)しかできない
- 強制アクセス制御(MAC)
  - システムポリシーをコンピュータ内で強制できる仕組み
    - たとえシステム管理者であっても、システムポリシーの回避や変更ができない

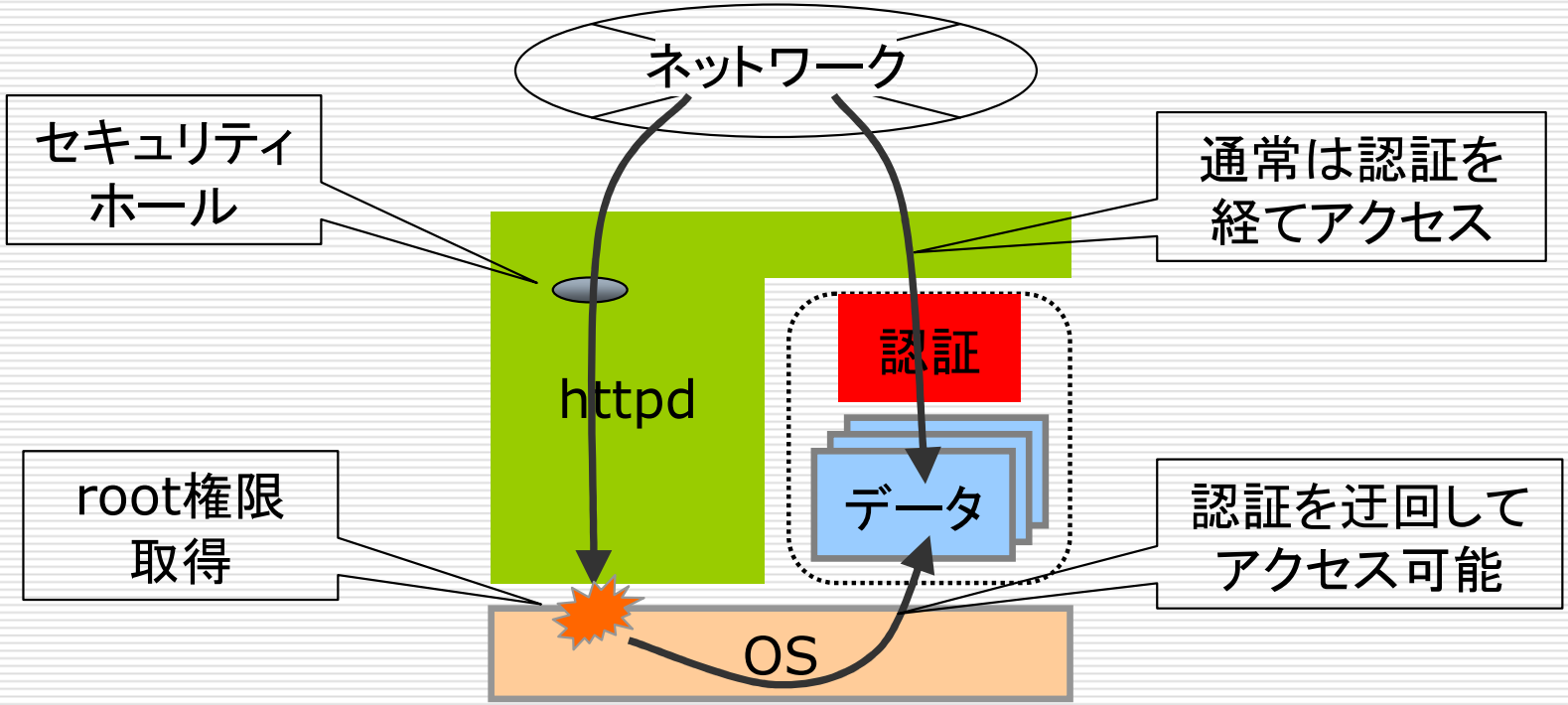
[システムポリシー]

ユーザのアクセス制限、プログラムの動作範囲を細かく設定する際のアクセス制御方針

参考:http://itpro.nikkeibp.co.jp/free/NC/NEWS/20040512/144041/

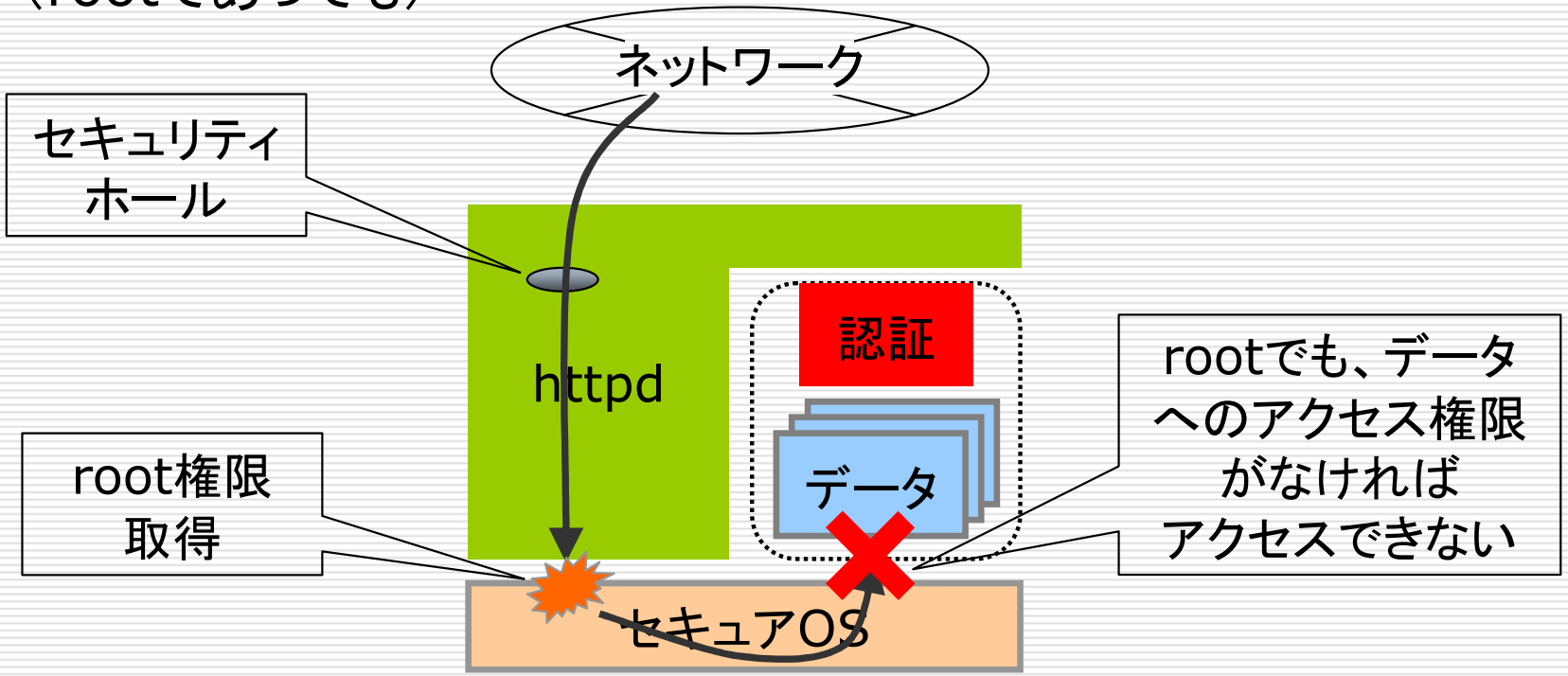
セキュアOSの利点

- 不正アクセスに対する防御
  - 機密情報、個人情報、コンテンツ保護
- 通常のOSの場合
  - root（管理者）権限をとれば何でもできてしまう



セキュアOSの利点

- 不正アクセスに対する防御
  - 機密情報、個人情報、コンテンツ保護
- セキュアOSの場合
  - システムポリシーに記述されたこと以外は何も出来ない（rootであっても）



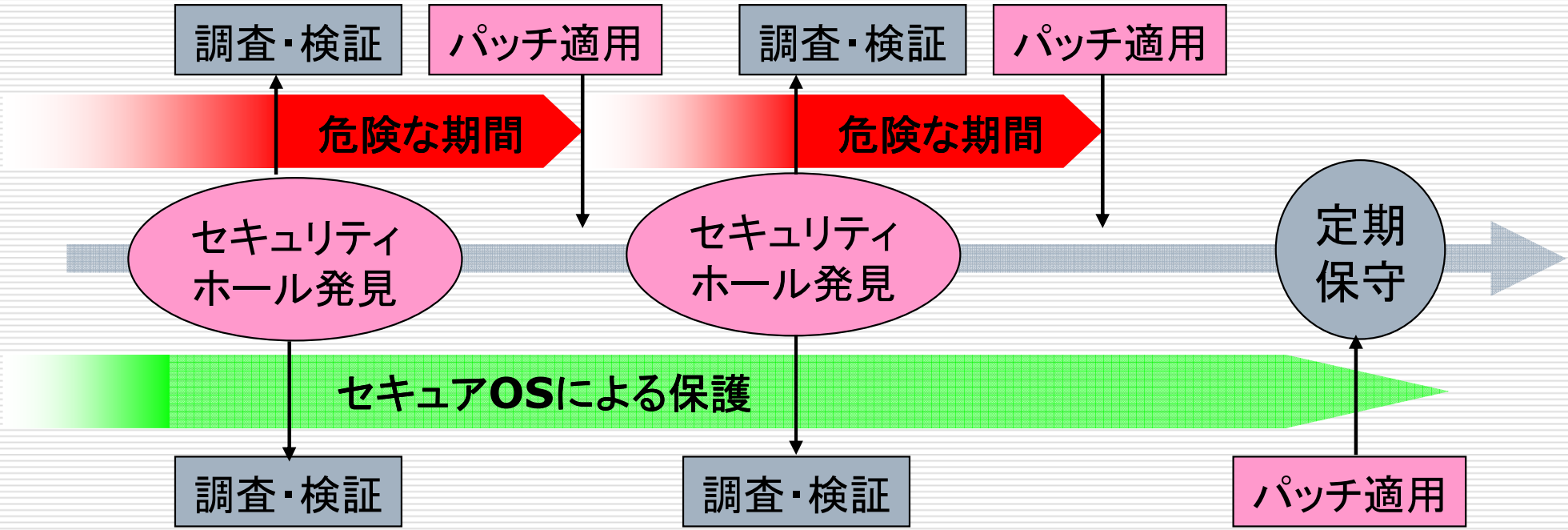
セキュアOSの利点（続き）

- 未知の脆弱性に対する耐性が高い
  - 0-day攻撃に対して強固
  - 脆弱性発見からパッチ適用までに時間的余裕
  - 組み込み機器では頻繁にアップデートを行うことができないものが多いため、重要
    - 情報家電
      - アップデートの徹底、回収が困難
    - 産業用途
      - 脆弱性があったとしても、正常に動作しているシステムにパッチを当てるのはリスクがある

        ・・・ もし動かなくなったら ・・・
      - 動作期間が長い（数年～10年以上の場合もあり）

産業用システムでの運用例

◆一般のOSによる運用



◆セキュアOSによる運用

- セキュアOSが不正な動きを封じることから、パッチを計画的に適用可能
- パッチ適用回数減少により、システム停止回数の削減可能

主なOSSのセキュアOS

SELinux

SELinux (Security-Enhanced Linux)

- NSA(米国国家安全保障局)で開発
- 非常に高度なセキュリティ機能
  - 設定粒度が非常に細かい
    - 設定が複雑でもある･･･
- Linuxカーネル2.6に標準実装
  - RHEL、Fedora Coreなどでデフォルト**ON**

SELinuxの機能

- TE (Type Enforcement)
  - プロセスには“ドメイン”、リソースには“タイプ” を割り当て（ラベル付け）
  - どのドメインがどのタイプにどのような操作が可能かを定義
    - パス名ではなく、貼り付けたラベルに基づくアクセス制御
- ドメイン遷移
  - あるドメインから子プロセスを起動して別のドメインとして動作させる
- RBAC (Role Based Access Control)
  - ロール（DB管理者、Web管理者など“役割”）に基づいたアクセス制御
  - ロール毎に使用可能なドメインを定義

組み込み機器とSELinux

- カーネルに標準で入っている
- ファイルシステムに左右される（inode内のxattr属性の有無）
  - 対応するファイルシステムが少ない（ext2/3,xfsなど）
    - 海外氏（NEC）によりJFFS2も使えるように（2.6.18以降）
- ユーザランドに手を加える必要
  - ps, ls, ・・・などでの属性情報表示の対応
  - BusyBoxの対応 → 後述
    - ドメイン遷移がうまく設定できない

組み込み機器とSELinux（続き）

- 機能が豊富すぎる？
  - 組み込み機器ではマルチユーザで使うことが少ない
    - RBACの機能はあまり必要ない
  - ポリシーの記述が複雑
    - タイプ付け→アクセス許可→ドメイン遷移→ロール設定
    - ポリシー記述の簡略化・サイズ縮小化が課題

      → 中村氏（日立ソフト）のSEEditの利用
  - MLS, MCS, ・・・

主なOSSのセキュアOS

LIDS

LIDS (Linux Intrusion Detection System)

- Xie Huagang氏とPhilippe Biondi氏により開発1999/10/15から公開
- 2005/12 面氏がLIDS Team入り

- 現在2.4系および2.6系のLinuxカーネルに対応
  - LIDS-1系列(1.2.x):Linux kernel 2.4用
  - LIDS-2系列(2.2.x):Linux kernel 2.6用
- カーネルにパッチを当てて利用

LIDSの機能

- ファイルのinode番号を使ったアクセス制御
  - 設定ではパス名を使う
- Linuxケーパビリティを使用した特権の分割
- BOOT, POSTBOOT, SHUTDOWN の3種の状態毎の設定
- カーネル保護（ブート後のモジュール組み込みの禁止）
- LIDSの運用に必要なコマンドは2つのみ
  - lidsadm
    - LIDSのシステム状態の管理を行う
  - lidsconf
    - アクセス制御の設定を行う（iptablesの記述に似ている）

組み込み機器とLIDS

- 適度な機能量
  - 場合によっては、権限分割の粒度が荒い
- 設定・理解が容易
- カーネルに対するパッチ
  - 量が少ないのでコードの理解はしやすい
  - ディストリのコードに当てるとサポートを受けられない問題
- ドメインの概念がない
- inodeによる問題
  - リンク先とリンク元の区別ができない → 特にBusyBox
  - inode番号の変化に注意が必要（ファイル更新時など）
  - ファイルシステムによってinode番号の割り当て方が異なる

主なOSSのセキュアOS

TOMOYO Linux

TOMOYO Linux

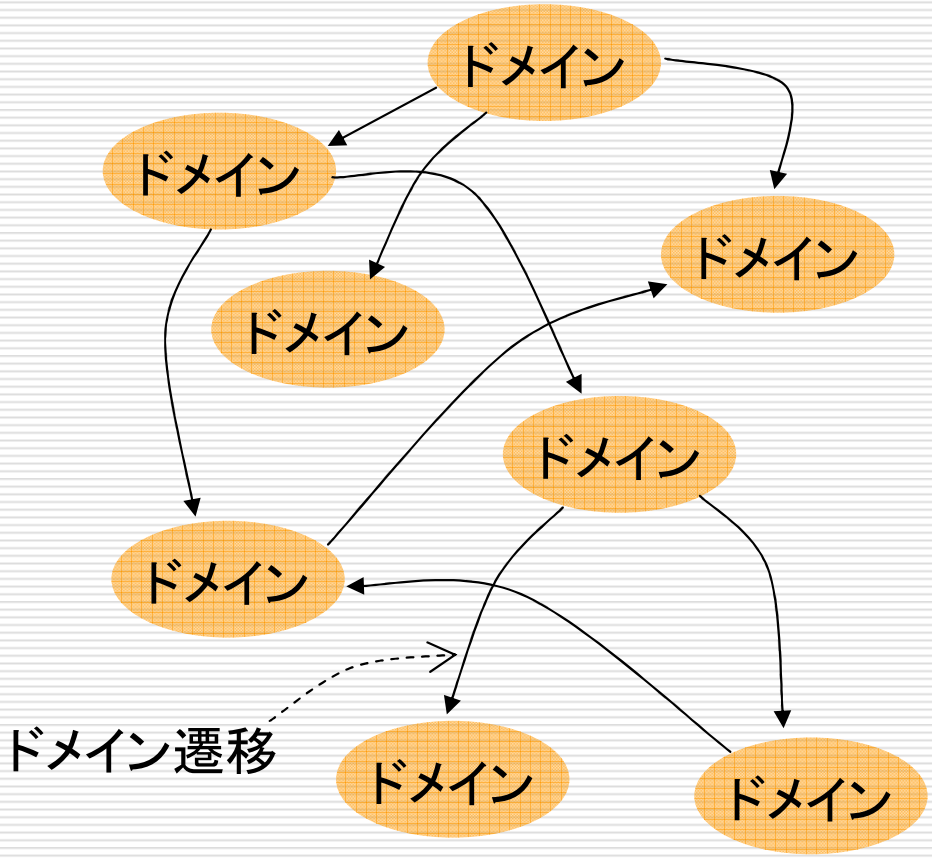
- （株）NTTデータで開発された、純国産のセキュアOS
- 2005年11月にオープンソースとして公開
- 現在バージョン 1.3.2
- LIDSと同じく2.4系および2.6系のLinuxカーネルに対応

TOMOYO Linuxの機能

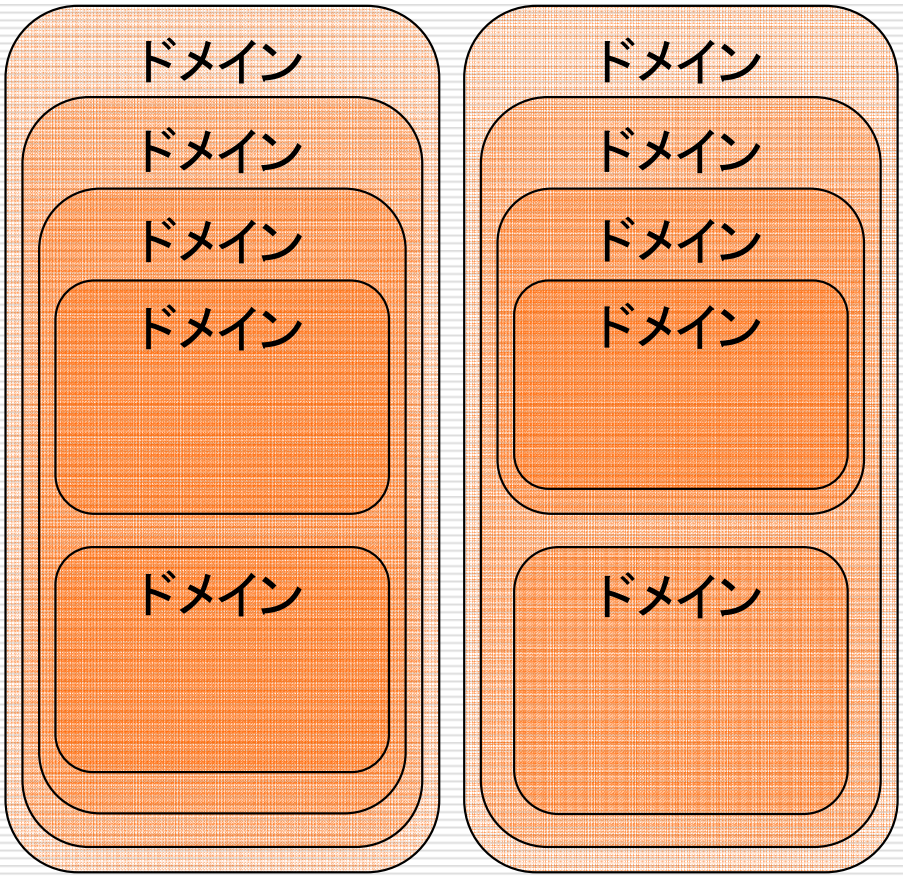
- パス名ベースのアクセス制御
- 自動学習機能
  - 他のセキュアOSにはない特徴的な機能
  - 学習モードにおいて実行・アクセスしたものの関係を学習し、運用モードでは学習したもの以外を拒否可能
  - 特にブート時、シャットダウン時のポリシー作成は非常に簡単・便利
  - ポリシーエディタを使うことで修正可能
- プロセスの呼び出し順序の履歴に基づくドメイン
  - bash → ls と、bash → bash → lsは別ドメイン
  - sshでログインしたbashと、コンソールからログインしたbashも別ドメイン
- 追加認証機能

SELinuxのドメインとの違い

- SELinux



- TOMOYO Linux



組込み機器とTOMOYO Linux

- 自動学習
  - 設定が非常に容易、柔軟
  - 必要最小限のファイルを抽出可能
- ファイルシステムの制限は無し
  - 純粋なパス名ベースのアクセス制御
- カーネルに対するパッチ
  - 量が少ないのでコードの理解はしやすい
  - ディストリのコードに当てるとサポートを受けられない問題
- リンク先とリンク元を区別可能
  - シンボリックリンクの場合は設定が必要
- 国内で開発している
  - 情報を集めやすい、意見を反映してもらいやすい

主なOSSのセキュアOS

3種の比較

比較表

	SELinux	LIDS	TOMOYO Linux
アクセス制御の細かさ	○	×	△
ポリシー記述の容易さ	×	○	△
自動学習	×	×	○
アクセス制御の基準	inode（ラベル）	inode（番号）	パス名
RBACの有無	○	×	△
ドメインの有無	○	×	○
組込系ファイルシステムとの相性	△	△	○
BusyBoxとの相性	×	×	○
対応カーネル	2.6（標準）	2.4, 2.6（パッチ）	2.4, 2.6（パッチ）

BusyBoxについて

BusyBoxとは？

- 沢山のコマンド（アプレット）を一つのバイナリにまとめ、コンパクトにしたもの
  - スイス・アーミー・ナイフのようなツール
- リンクを張って使用する
  - **Ex.)**

ln –s /bin/busybox /bin/ps
ln –s /bin/busybox /bin/vi
ln –s /bin/busybox /sbin/fdisk

- 共通コードをまとめて、フットプリントを小さくできる

```
~ # busybox
BusyBox v1.2.2 (2006.10.31-00:55+0000) multi-call binary

Usage: busybox [function] [arguments]...
   or: [function] [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as!

Currently defined functions:
        [, [[, addgroup, adduser, ash, basename, busybox, cat, chgrp,
        chmod, chown, chroot, clear, cmp, cp, cut, date, dc, dd, delgroup,
        deluser, df, dirname, dmesg, du, dumpleases, e2fsck, echo, egrep,
        env, expr, false, fdisk, fgrep, find, free, fsck, fsck.ext2, fsck.ext3,
        getopt, getty, grep, gunzip, gzip, halt, head, hexdump, hostid,
        hostname, httpd, hwclock, id, ifconfig, ifdown, ifup, inetd, init,
        insmod, kill, killall, klogd, less, ln, logger, login, logname,
        ls, lsmod, md5sum, mkdir, mke2fs, mkfs.ext2, mkfs.ext3, mknod,
        mkswap, modprobe, more, mount, mv, netstat, nslookup, passwd,
        pidof, ping, pivot_root, poweroff, ps, pwd, rdate, reboot, reset,
        rm, rmdir, rmmod, route, run-parts, sed, sh, sha1sum, sleep, sort,
        strings, stty, su, swapoff, swapon, sync, syslogd, tail, tee,
        telnet, telnetd, test, time, top, touch, true, tty, udhcpc, udhcpd,
        umount, uname, uniq, uptime, usleep, vi, wc, wget, which, whoami,
        xargs, yes, zcat

~ #
```

セキュアOSとBusyBoxの相性

- TOMOYO Linux
  - 問題なし！
- LIDS
  - アプレットごとにアクセス制御が設定ができない
- SELinux
  - アプレットごとにドメイン遷移が設定ができない
  - ls、psなど属性情報表示の対応が十分でない

最初はシンボリックリンク未対応。

自分のブログにTOMOYOでBusyBoxを使ったことを書いておいたら、いつの間にか対応！

BusyBoxとLIDS

- /bin/busyboxを呼び出すバイナリを作成（バイナリラッパ）
  - Cで書くとこんな感じ

```
void main(int argc, char* argv[], char* envp[]) {
    argv[0] = "cat";
    execve("/bin/busybox", argv, envp);
}
```

  - これをアセンブラで記述（サイズは1k未満）

```
/bin # ls -l
-rwxr-xr-x    1 root     root           696 Aug 17 12:01 addgroup
-rwxr-xr-x    1 root     root           692 Aug 17 12:01 adduser
-rwxr-xr-x    1 root     root           688 Aug 17 12:01 ash
-rwxr-xr-x    1 root     root           688 Aug 17 12:01 cat
-rwxr-xr-x    1 root     root           692 Aug 17 12:01 chgrp
...
```

- アーキテクチャ毎にコードをメンテナンスする必要

参考：「BusyBoxを使った組み込み機器でLIDSを動かすには」（佐藤 祐介氏）
http://www.selinux.gr.jp/LIDS-JP/document/general/web_lids_busybox/main.html

BusyBoxとSELinux

- BusyBoxには以前からSELinuxオプションがあった・・・
  - でもほとんどメンテナンスされてなかった
- 海外氏、中村氏を中心に、ユーザ会有志で“SELinux/BusyBox Project”を立ち上げ
  - http://www.kaigai.gr.jp/index.php?busybox
  - 通称、”se-busybox”
  - ls、cp、mvなどcoreutils関連のSELinux対応
  - SELinux関連コマンドのBusyBox化
    - matchpathcon, setenforceなどなど

SELinux関連コマンドのBusyBox化

- これまでの状況
  - 2006/11
    - プロジェクト立ち上げ
  - 2007/02
    - libselinux関連コマンドがBusyBox本家にマージ
      - getenforce, getsebool, matchpathcon, selinuxenabled, setenforce
  - 2007/03
    - coreutils関連SELinux対応が本家にマージ
      - cp, ls, mkdir, mknod, mv, id, install, mkfifo, stat, chcon, runcon

BusyBoxのドメイン遷移

- アプレットのドメイン遷移問題
  - 解決手段
    - カーネル拡張 → 現実的でない
    - バイナリラッパ → あまり現実的でない（メンテの問題）
    - BusyBoxの拡張
      - 内部でアプレット呼び出し時にドメイン遷移
        - BusyBoxのコアに手を加える必要がある（作業中）
      - BusyBox自体に脆弱性があった場合、被害が大きくなることがある
    - スクリプトラッパ
      - “#!/bin/busybox”と一行書いたスクリプトファイルで呼び出す
        - http://d.hatena.ne.jp/hshinji/20070221
      - 通常のSELinuxの動作に従ったドメイン遷移が可能
      - ただし、BusyBoxの/bin/shによるシェルスクリプトが動かない（execve(2)の制限）
  - 現状は、①スクリプトラッパ ②BusyBoxの拡張 という感じ
- その他の解決案検討中＆募集中

最後に

まとめ

- LIDSは組み込み機器で実績がある
  - 分りやすさ&コンパクト
  - ただ、LIDS自体の開発が停滞気味･･･
- TOMOYO Linuxが現状ではもっとも組み込み向き？
  - 自動学習機能が強力
  - メインラインに含めるため、国際舞台に打って出るところ
    - CELF@San Jose, California (4/17～19)
- SELinuxも組み込み機器対応に向けて着々と
  - Linuxカーネルに標準＆機能的に有利
  - BusyBoxのSELinux対応
  - ポリシーサイズの改善が課題
    - “SEDiet”という取り組みが進行中

参考リンク

- SELinux
  - 本家　http://www.nsa.gov/selinux/
  - 国内　http://www.selinux.gr.jp/
- LIDS
  - 本家　http://www.lids.org/
  - 国内　http://www.selinux.gr.jp/LIDS-JP/
- TOMOYO Linux
  - http://tomoyo.sourceforge.jp/
- Busybox
  - 本家　http://busybox.net/
  - SELinux/BusyBox Project
    http://www.kaigai.gr.jp/index.php?busybox

ご清聴ありがとうございました